Foundation – Module 2

ELO 2.1 Match foundational cloud terms from the section to appropriate definitions;

ELO 2.2 Identify three cloud service models and a representative example of each;

ELO 2.3 Identify public, private, community and hybrid cloud deployment models, and a representative example of each;

ELO 2.4 Identify risks associated with using a Cloud solution for DoD mission-owner's requirement;

ELO 2.5 Recognize there are several different information impact levels related to DoD data (PII, PHI are different from public facing information; shades of grey in CUI).

Module – 2: Foundation

Topics

- Module Introduction
- Overview of Cloud Computing
  - Characteristics
  - Service Models
  - Deployment Models
- Risks to using Cloud
- Information Impact Levels
- Module Review
- Module Summary Questions

You should be able to:

- Identify three cloud service models and a representative example of each.
- Identify public, private and hybrid cloud deployment models, and a representative example of each.
- Match foundational cloud terms from the section to appropriate definitions.
- Identify risks associated with using a Cloud solution for DoD mission-owner's requirement
- Recognize there are several different information impact levels related to DoD data (PII, PHI are different from public facing information; shades of grey in CUI).

Recapitulation of Module - 1

Topic

Review Previous Content

You should be able to:

Questions

Content

- Identify three advancements in technology that enabled the rise of cloud computing (marketing concept).
- benefits of consuming cloud services;
- characteristics of a cloud service;

Overview of Cloud Computing

Topic

Overview of Cloud Computing

You should be able to:

1. Identify 5 Characteristics of a cloud service
2. Identify 3 Cloud Service Models

Questions

1. Cloud computing, as defined by the National Institute for Standards and Technology, is a model for enabling ubiquitous, convenient, _____ network access to a _____ _____ of configurable computing resources that can be _____ provisioned and _____ with minimal management effort or service provider _____.
2. What are the 3 NIST identified cloud service models?

Content

- Cloud computing, as defined by the National Institute for Standards and Technology (NIST), is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST, 2011)
- This definition outlines the five essential characteristics,
  - on-demand self-service,
  - broad network access,
  - resource pooling,
  - rapid elasticity,
  - measured service;

Characteristic: on-demand self-service

Topic

On-Demand Self-Service

You should be able to:

Questions

1. What are the two attributes for provisioning On-Demand Self-Service computing capabilities with a cloud service provider? Unilaterally and automatically without human interaction.

Content

- With on-demand self-service, a consumer can unilaterally provision computing capabilities automatically without requiring human interaction with a cloud service provider. (NIST, 2011) Capabilities such as server time and network space are acquired through a web-based control panel. In this automated setting, the cloud service provider (CSP) cannot assume specialized technical knowledge on the consumer's part. Therefore, the provider should design an understandable user interface with settings that make sense to a non-technical user. (Sinnema, On Demand Self-Service, n.d.)
- The self-service capability allows the information technology (IT) labor force to focus less on collecting customer requirements and more on planning and designing new capabilities.

Characteristic: broad network access

Topic

Broad network access

You should be able to:

Questions

1. According to NIST, Broad network access refers to cloud computing resources being accessible over the network through any standard heterogeneous client platform such as mobile phones, tablets, laptops and desktop computers.

Content

- Broad network access refers to cloud computing resources being accessible over the network through any standard heterogeneous client platform such as mobile phones, tablets, laptops and desktop computers. (NIST, 2011) Consumers can use these devices to access the cloud from any location via a simple web-based access point. Standardized services and web implementations allow customers to access cloud resources from a variety of devices and applications. (The Open Group, 2013)
- A popular example of this characteristic is a consumer's ability to access web-based email, such as Gmail and Yahoo, from any device. This mobility is especially advantageous to consumers who frequently need to access information while mobile or from a telework location.

Characteristic: resource pooling

Topic

Resource Pooling

You should be able to:

Questions

1. Major Take-Aways: Resource pooling may introduce security concerns because the consumer typically has no control over where their data is stored or with whom resources are shared.

Content

- With resource pooling, the cloud service provider's computing resources are pooled to serve a large number of simultaneous consumers. Different physical and virtual resources, such as storage, processing, memory, and network bandwidth, are dynamically assigned according to consumer demand. (NIST, 2011) Pooling resources builds economies of scale, which in turn lowers costs for consumers. It also removes inhibitors from the environment and increases efficiency by reducing crowding. (Benson, 2013)
- However, resource pooling may introduce security concerns, because the consumer typically has no control over the location of the provided resource or knowledge of other organizations that are sharing the resource. For data security, performance, and compliance with regulations, consumers may be able to specify their computing resource location generally, such as by country, state or data center. (The Open Group, 2013)

Characteristic: rapid elasticity

Topic

Rapid Elasticity

You should be able to:

Questions

Content

- Elasticity is the capability for an enterprise to scale up and down their operations within a cloud environment. (He & L. Guo, 2011) Computing capabilities can be flexibly provisioned and released, in some cases automatically, to rapidly scale up and down in accordance with consumer demand. (NIST, 2011)
- Resource pooling helps providers achieve elasticity because different services running on the cloud can have different workload patterns (seasonal, batch, etc.), and these differences allow the provider to balance the workload. (Sinnema, Rapid Elasticity, n.d.)
- Furthermore, the available capabilities appear unlimited to the user and can be accessed in any quantity, at any time.(NIST, 2011)
- The ability to scale at will requires providers to dynamically provision new computing resources based on demand monitoring. (Sinnema, Rapid Elasticity, n.d.) In combination with the pay-per-use billing model, the elasticity of the cloud provides consumers with significant savings.
- A common example of this is a retail web site(like amazon.com) that is accustomed to a consistent number of customers. However, a sudden rise in product popularity will increase the traffic significantly.
- If the site is hosted on a traditional, dedicated server, the lack of resources could cause the site to become unreachable. However, if hosted in the cloud, the resources could be rapidly scaled up to meet the rise in demand.

Characteristic: measured service

Topic

Measured Service

You should be able to:

Questions

Content

- Cloud service providers automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service. Measuring resource usage can provide transparency for both the provider and the consumer. (NIST, 2011)
- This is especially important for the pay-per-use billing model because consumers need sufficient measurements to make purchasing and operational decisions. (The Open Group, 2013) Every aspect such as central processing unit (CPU) performance, memory utilization, and network bandwidth is measured so as to deliver precisely configured services to the consumer. (Benson, The Cloud Defined: Measured Service, 2013)
- On the provider end, measurability goes hand in hand with rapid elasticity, allowing providers to dynamically provision new computing resources to meet rapidly changing consumer needs.

Service Models: Overview

Topic

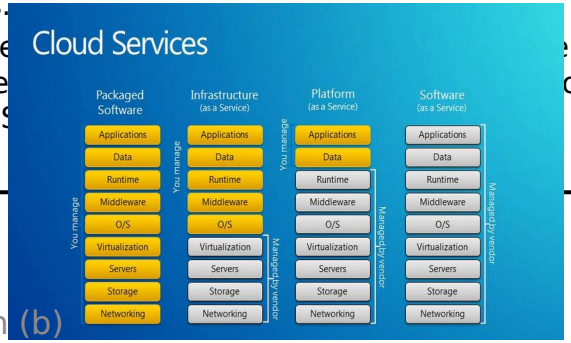
Overview of Service Models

You should be able to:

Questions

Content

- NIST defines three models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
- Unlike package software, these models help differentiate the implementation responsibilities that fall on the CSP from the responsibilities that fall on the customer.
- Each service model serves a different need and provides a different level of capability to an organization.
- Although not specified by NIST, the Anything as a Service (*aaS) nomenclature has created niche markets for delivery of specialized tools and capabilities (What is XaaS, 2010).
- For example, Disaster Recovery as a Service (DRaaS) allows organizations to outsource their business continuity capabilities so that they do not need to invest in their own dedicated alternate sites. Monitoring as a Service (MaaS) allows organizations to leverage dedicated cybersecurity professionals who can watch for intrusions and malware across all of their client's networks.
- These spe emerging and there ons as do IaaS, PaaS



(b)

Service Model: Infrastructure

Topic

Infrastructure as a Service

You should be able to:

Questions

Content

- **NIST Definition**: "[Provisioning] processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."
- **Example**: Amazon Web Services, Microsoft Windows Azure

(Note to developer, we clude CSP w/ DOD PAs)

Service Model: Platform

Topic

Platform as a Service

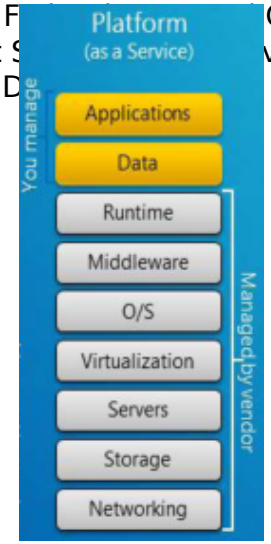
You should be able to:

Questions

1. Major Take-Away.

Content

- **NIST Definition**: "[Deploying] onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment."
- **Example**: Oracle F Cloud Services, Micropact Product S veloper, we may want to include CSP w/ D



Service Model: Software

Topic

Software as a Service

You should be able to:

Questions

Content

- **NIST Definition**: "[Using] the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration setti
- **Examples:** Googl Concur
- (Note to develope o include CSP w/ DOD PAs)

Deployment Models: Overview (1)

Topic

Deployment Models: Overview (1)

You should be able to:

1. Colocation
2. Physical Isolation
3. Physical Separation
4. Logical Separation

Questions

1. Within a data center, the space the tenant rents is physically isolated, or caged-off, from the other tenants in the facility
2. If a data center rents its resources to more than one tenant, the location has multi-tenancy.
3. Cloud Service Providers (CSPs) have data centers where separate physical IT infrastructure is operated for their cloud service offering (CSO).
4. Instead of floor space, CSPs rent a portion of their cloud service offering's capacity, which is sometimes called a Virtual Private Cloud (VPC)
5. VPCs are not physically separated, but instead have logical separation.
6. Cloud service provider's capacity, when divided amongst many tenants, results in logical separation of the data.
7. Physical separation is when CSPs are able to cage-off portions of their data centers to operate the physical IT infrastructure for multiple cloud service offerings.

Content

- Before getting into the topic of Deployment models it would be helpful to take a step back.
- Today, there are many companies, known as Co-location Providers (or COLOs) who have buildings (**data centers**) that provide resources such as physical security, power, cooling, and network connectivity. The COLO then **rents** floor-space to other businesses (**tenants**) who in turn install, manage, and maintain their own IT infrastructure and software applications. The space that the tenant rents is **physically isolated** (**caged-off**) from the other tenants in the facility in much that same way that public storage facilities rent space to people who want to store their "stuff." A COLO is a classic example of **multi-tenancy** – e.g. many businesses share/rent the resources provided by the land-lord.
- In the case of the CSP … they too have data centers where they house and operate the physical IT infrastructure for their cloud service offering. However, instead of renting floor space, they sell a portion of their CSO's **capacity**; which you might hear called 'virtual private cloud' (VPC), 'virtual private data center' (VDC), etc., the ideas are the same.
- Two important points to understand: Unlike the COLOs, the VPCs are not physically separated – This is known as **logical separation.** Like the COLO, the CSP is able to cage-off portions of their data cetner to operate the physical IT infrastructure for their cloud service. This is known as **physical separation**.
- Multi and single tenancy and physical and logical separation become especially important when we start talking about risks and cybersecurity.

Deployment Models: Overview (2)

Topic

Deployment Models: Overview (2)

You should be able to:

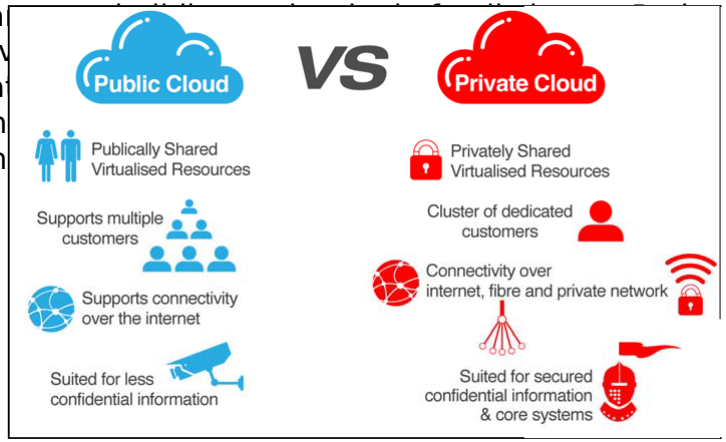
1. Public
2. Private

Questions

1. What are the two most prevalent cloud service models? Public and Private
2. What customer needs may dictate which cloud service model they may choose? Security, privacy and cost.

Content

- Cloud services can be deployed in different ways depending on the customer's specific needs, such as security, privacy, and cost.
- The two most prevalent models are Public Cloud and Private Cloud as depicted below. The same technical capabilities of cloud are provided in either model; however, the main difference between the two models is access: Public Clouds are open to all users (multi-tenant) – Private Clouds are closed to all users except the users identified by the Business Entity paying for the service (single-tenant).
- A common way of thinking about public vs. private is an apa
  prov
  hea
  fam
  fam


Public Cloud
VS
Private Cloud
Publically Shared Virtualised Resources
Supports multiple customers
Supports connectivity over the internet
Suited for less confidential information
Privately Shared Virtualised Resources
Cluster of dedicated customers
Connectivity over internet, fibre and private network
Suited for secured confidential information & core systems

Deployment Models: Overview (3)

Topic

Deployment Models: Overview (3)

You should be able to:

1. Competition for resources

Questions

1. What are the four deployment models defined by NIST? Public, private, community and hybrid.
2. True or False, regardless of the cloud being Public or Private, the behavior of one tenant in a cloud deployment model may adversely affect other tenants?

Content

- Building on the home apartment analogy, you should be able to extend the idea that in any cloud, all the physical resources supporting the delivery of the cloud service offering are shared among the various tenants and/or consumers of the CSO.
- Looking to NIST once again, we will now define the four deployment models.
- NIST identifies four deployment models
  - Public,
  - Private,
  - Community,
  - and Hybrid.
- This means, regardless of the cloud being Public or Private, that the behavior of one tenant may adversely impact other tenants. For example, we know that one physical server is able to support many virtual servers; however, if one of the virtual servers is consuming a large amount of CPU that will likely cause the other virtual servers to receive less capacity from the underlying physical CPU.

Deployment Model: Public

Topic

Public Cloud

You should be able to:

1. Identify the public deployment model NIST definition.

Questions

Content

- Public cloud infrastructures operate in a multi-tenant environment whose resources are allocated for the general public. Public clouds tend to be large and provide economies of sale for their customers.
- However, security and privacy concerns are heightened because any individual or organization can potentially access the same cloud infrastructure.
- For example, there is an high-quality CSO that is being marketed as being designed to allow US government agencies and customers to move sensitive workloads to the cloud. This is an example of a Public Cloud that is managed and has been configured to provide additional measures to restrict users to those that are U.S. Persons.
- As we will learn, there are ways for DoD to assess the CSO for fitness for use in hosting and processing DoD data and applications. Suffice it to say at this point and even though additional measures have been put into place, this CSO should only be used to host DoD information that has been approved for public release such as public facing web sites.
- We will also learn that there are many subtle and not-so-subtle risks that need to be considered when using a CSO. For example, what potential risk might there be to the DoD Information Network if an outbound network connection were made to a web server offered by this CSP? What would happen if an hacker were able to deface or change the content on the web server offered by this CSP?

Deployment Model: Private

Topic

Private Cloud

You should be able to:

Questions

1. What is one potential drawback of a private cloud? Cost
2. Identify an example of a DoD private cloud. milCloud
3. True or False, DoD must assess a Cloud Service Offering for fitness for use in hosting and processing DoD data and applications before it can use it.
4. What are some advantages to having a private cloud? Private clouds can offer very high levels of security and access control making them better suited for applications and data where impact to the DoD mission is a primary consideration.

Content

- Private cloud infrastructures are operated only for an individual organization. The organization can leverage the scalability and performance aspects of cloud computing, but the infrastructure is isolated from that of other organizations, improving security and privacy.
- Because of their specialized nature, private clouds could potentially be as costly as dedicated data centers.
- For example the DoD has a Private Cloud, milCloud which is a multi-tenant IaaS operated by DISA isolated to SIPRNet and NIPRNet. However, the DoD wants to leverage commercial innovation and encourage open competition; other commercial offerings are-and-will-be under evaluation that are expected to support the IaaS, PaaS, and SaaS models.
- As we will learn, there are ways for DoD to assess the CSO for fitness for use in hosting and processing DoD data and applications. Private Clouds can offer very high levels of security and access control making them better suited for applications and data where impact to the DoD mission is a primary consideration.

Deployment Model: Community

Topic

Community Cloud

You should be able to:

1. Identify that a Community cloud deployment model is just a specific type of private cloud provisioned for a specific community of interest.

Questions

1. A community cloud is just a specifically provisioned private cloud.
2. Community cloud infrastructures are private clouds provisioned for a specific community of interest with shared concerns.

Content

- Community cloud infrastructures are private clouds provisioned for a specific community of interest with shared concerns, such as a government-only cloud.
- As described earlier, DISA's milCloud is intended to supports a very broad community, the DoD. There are other Private Clouds within the DoD that are meeting specific mission and/or application needs, however, they have yet to (and never may be) merged into a Community Model as envisioned by NIST.
- The Departments current focus is on leveraging commercial cloud services to the maximum extent possible which argue for investing in Hybrid Cloud rather than attempting to build, operate, and maintain several DoD Private Clouds.

Deployment Model: Hybrid

Topic

Deployment Model: Hybrid

You should be able to:

Questions

1. By combining a private cloud and a public cloud, the result is a hybrid cloud.
2. True or False, a single cloud deployment model is able to meet all the unique requirements of the DoD? False

Content

- Hybrid cloud infrastructures are combinations are any two or more of the other cloud infrastructures.
- For example, combining a private cloud and public cloud.
- This model will be the most prevalent model for the DoD given its strategy to aggressively pursue the competitive acquisition and use of commercial cloud service offerings and understanding that “one cloud’ will not meet all the unique requirements of the DoD.
- One example of Hybrid Cloud is the Development – Test – Production software lifecycle. It has been shown that development and test (e.g. development testing and limited operational testing) can take place in a commercial CSO with greater flexibility and at lower cost and once complete the application can be run in production in milCloud.
- Combining cloud infrastructures is not the only way to think of hybrid cloud. Recall that cloud service offering is provided by a cloud service provider. By definition a CSP is the business entity that is selling the offering; however, they may not be the only entity involved in providing the offering. There are examples where CSPs develop an application selling it as a SaaS. When looking under the covers they could be acquiring the IaaS to run the application from a third party.
- Combining cloud infrastructures presents a variety of cybersecurity concerns that require careful analysis of how the CSOs are architected, deployed, assessed, and authorized.

Risks to DoD Mission Owners

Topic

Areas of Risk

You should be able to:

1. ELO 2.4 Identify risks associated with using a Cloud solution for DoD mission-owner's requirement;

Questions

Major Take-Away: Overall mission risk will be assessed and authorized by the mission owner's Authorizing Official (AO) through the issuance of an Authority to Operate (ATO).

There is risk to data and risk to the DoD Information Network (DoDIN)

Content

- This section will provide an over-view of the risks to a DoD MO when utilizing a CSO.
- Overall Mission will be assessed and authorized by the Mission Owner's Authorizing Official (AO) through the issuance of an Authority to Operate (ATO). Mission refers to the information system and functions for which a DoD entity acquires or uses a CSO. Understanding the distinction between what's provided and addressed with the CSO versus what's addressed by the Mission Owner is critical to implementing the DoD cloud security requirements.
- Risk to Data – Information Impact Level
- Risk to DoDIN

Risks to DoD Mission Owners

Topic

Risks to DoD Mission Owners

You should be able to:

1. ELO-085 Recognize there are several different information impact levels related to DoD data (PII, PHI are different from public facing information; shades of grey in CUI).

Questions

1. How many Information Impact Level does the 12 January 2015 Cloud Security Requirements Guide define? 4
2. True or False, according to the Cloud Computing Security Requirements Guide, a DoD Mission Owner can

Content

- The January 12, 2015 Cloud Computing Security Requirements Guide (SRG) describes 4 information impact levels.
- We will get more into the specific Information Impact Levels in Module 5 when we look at Assessment and Authorization of a Cloud Service Offering.
- Suffice it to say, there are different controls that must be applied to DoD data depending upon the information impact levels.
- There is Non-Controlled Unclassified Information which includes all data cleared for public release, as well as some DoD private unclassified information not designated Controlled Unclassified Information or critical mission data, but the information requires some minimal level of access control.
- There is also Controlled Unclassified Information which contains a number of categories, including but not limited to, export control, privacy information, such as Personally Identifiable Information (PII), Protected Health Information, as defined in the Health Insurance Portability and Accountability Act (HIPA), and other information requiring explicit CUI designation (i.e. For Official Use Only, Law Enforcement Sensitive, Critical Infrastructure Information, and Sensitive Security Information).
- There is a higher Information Impact Level for CUI that requires even more protection as deemed necessary by the information owner, public law, or other government regulations. It can support unclassified National Security Systems.
- The fourth Information Impact Level can accommodate information that has been determined to be classified national security information up to the SECRET level.

Module 2 - Review

Topic

Summary

Content

You should be able to:

Questions

Module 2 – Summary Questions

Topic

Summary

Content

You should be able to:

Questions